IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF DEVICES SEIZED PURSUANT TO SW-20-mj-213-01-AJ, NOW SECURED IN THE CUSTODY OF THE FBI, AS DESCRIBED FULLY IN ATTACHMENT A	Case No. 20- mj-214-AJ

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Tarah Rankins, a Special Agent with the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state as follows:

1. I have been employed as an FBI Special Agent since 2015, and am currently assigned to the Boston Field Office, Bedford Resident Agency. I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber-crime, child exploitation, and child pornography. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the devices seized from the person and premises of Stuart Adams ("SUBJECT DEVICES"), described fully in Attachment A, for the things described in Attachment B – specifically, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(4)(B), which relates to the illegal

possession of child pornography, and Title 18 United States Code. Section 2252A(a)(2), which relates to the illegal receipt of child pornography.

3. During the course of this investigation I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. §§ 1470, 2252(a)(4)(B), and 2252A(a)(2), related to the possession and receipt of child pornography in the District of New Hampshire. 18 U.S.C. § 1470, makes it a crime for anyone, using the mail or any facility or means of interstate or foreign commerce, to knowingly transfer or attempt to transfer obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years. 18 U.S.C. § 2252(a)(4)(B) makes it a crime for any person to knowingly possess one or more images depicting a minor under the age of 18 engaged in sexually explicit conduct. 18 U.S.C. § 2252A(a)(2) makes it a crime for any person to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

6. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

7. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

8. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook"

computers).

9. Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an internet service provider assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

10. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

11. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

12. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory

calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

13. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

14. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

PROBABLE CAUSE

15. On August 22, 2020 a source who has previously provided reliable information to the FBI pertaining to online child exploitation offenses contacted the FBI regarding Kik, a mobile application that allows users to send each other messages that include text, pictures and videos[1]. The source, who maintains a presence on Kik, stated that the Kik username " 3003", with a display name of Steve A ("SUSPECT KIK USER") and email address of @yahoo.com" was a 59 year-old male that expressed to the source an interest in chatting

[1] According to the publicly available "Kik's Guide for Law Enforcement", Kik is a smartphone messenger application that lets users connect with their friend and the world around them through chat. Users can send text, pictures, and videos and more – all within the app. Kik is available to download through iOS App Store and the Google Play store on most iOS (iPhone/iPod/and iPad) and Android (including Kindle Fire) devices. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can send each other text messages, images, and videos. "Kik's Guide for Law Enforcement" is available at https://lawenforcement.kik.com/hc/en-us//articles/360039841472-Law-Enforcement-Guide.

with underage females. On numerous occasions, the SUSPECT KIK USER requested that the source help him establish contact with minor females on the Kik platform.

16. On October 6, 2020, at the direction of the FBI, the source provided the SUSPECT KIK USER with the Kik username, "the online persona of an FBI Online Undercover Employee ("OCE") portraying a 13-year-old girl. The OCE was engaged in an online operation designed to identify adults who were seeking out minors online for sexually explicit conduct. The source advised the SUSPECT KIK USER that " was a 13-year-old girl named Madison living in the United States. Soon after, the OCE received a message on Kik from the SUSPECT KIK USER who introduced himself as "Steve." The SUSPECT KIK USER and OCE then chatted exclusively on the Kik messenger application. The SUSPECT KIK USER revealed to OCE that he lives in New Hampshire. OCE responded that she lives in Massachusetts.

17. Thereafter, the SUSPECT KIK USER and the OCE communicated regularly through private messages on Kik throughout October and November 2020. The chats were always initiated by the SUSPECT KIK USER and frequently included discussion of sexual topics. During several chats, the SUSPECT KIK USER sent the OCE images and/or videos that purported to depict his own unclothed, erect penis. The following chat, which took place on the afternoon of October 15, 2020, is demonstrative:

SUSPECT KIK USER: Hmm, I'm back at my desk. No pants this time.

OCE: No????. [Surprised Emoji]. Boxers?

SUSPECT KIK USER: Sorta..boxerbriefs. Should I just those off too

OCE: Mmm

SUSPECT KIK USER: Should I

OCE: Errmmm….If u want to!! [Smiling Emoji with Heart Shaped Eyes]

SUSPECT KIK USER: Okay …slipping them off

OCE: [Smiling Emoji]

SUSPECT KIK USER: What about you?

OCE: Are they off?!

SUSPECT KIK USER: Yep

OCE: My mom is in the other room [Upset Emoji]

SUSPECT KIK USER: Oh okay..oops. What are you wearing now

OCE: No it's ok! I just can't rn [Disappointed Emoji]. Are urs really off?!

SUSPECT KIK USER: Yeah ..just in tshirt and socks

OCE: And what r u doin????

SUSPECT KIK USER: Chatting with you [Smiling Emoji]. What are you suggesting.

OCE: Lol that's it?? Idk. U have no pants [Blushing Emoji]

SUSPECT KIK USER: Well touching a little

OCE: [Smiling Blushing Emoji]

SUSPECT KIK USER: Oh….you like that

OCE: Maaayyyybe [Kiss Emoji]

SUSPECT KIK USER: Maybe?

OCE: Yessss

SUSPECT KIK USER: Oh my..thinking of you

OCE: Yea??

SUSPECT KIK USER: What if you were here

OCE: What r u thinking about?

SUSPECT KIK USER: Thinking about you touching me

OCE: [Smiling Emoji]

SUSPECT KIK USER: You told me you had only touched one guy

OCE: I would like that. Yes. Is that ok?

SUSPECT KIK USER: Good. Yes,it is

OCE: Ok phew

SUSPECT KIK USER: Would be nice

OCE: Is it hard??!

SUSPECT KIK USER: Yes very

OCE: [Surprised Emoji]

SUSPECT KIK USER: I'm bigger than your ex

OCE: Really?! I'm sure But he is just a boy. Only one I've seen [Sad Emoji]. I feel other girls in my grade have seen more.

SUSPECT KIK USER: Yes I'm sure. Why do you say that

OCE: Just what I've heard. Is it still hard????

SUSPECT KIK USER: Yes

OCE: [Smiling Emoji with Heart Shaped Eyes]

SUSPECT KIK USER: You want to see?

OCE: Errmmmm…..yesssssss

SUSPECT KIK USER: [Sends a picture of a naked adult erect penis from an overhead camera angle. The picture also depicts a tan rug/mat with a black and red checkered border on the floor.][2]

SUSPECT KIK USER: Only fir you

OCE: [Four Heart Emojis]

SUSPECT KIK USER: Oh you like it?

18. Records obtained from Yahoo provided subscriber information for email address @yahoo.com' provided a verified telephone number associated with the subscriber information to be 4241 and a Registration IP address of 73.142.155.80.

19. Records obtained from Verizon indicate that the telephone number 4241 is associated with an account held in the name of Stuart L. Adams, with a current billing address of Hooksett, New Hampshire 03106 (the SUBJECT PREMISES).

20. Records obtained from Kik from 10/6/2020 – 11/16/2020 for username " 3003" show a Registration IP address of 73.142.155.80.

21. Records obtained from Comcast for the subscriber of the IP address 73.142.155.80 from August 2020 through November 2020 confirm that the IP address is assigned to Stuart Adams, with a service address of Hooksett, NH 03106.

22. Through an inquiry of the New Hampshire Department of Safety – Division of Motor Vehicles ("DMV") database, the FBI was able to further identity Stuart L. Adams's year

[2] This image is available for the Court's review.

of birth as 1961, making him 59 years old, as well as the residence of Adams as Hooksett, New Hampshire 03106, near Manchester, New Hampshire.

23. I reviewed the photograph of Adams in the DMV database, as well as the photographs or "profile picture," associated with the SUSPECT KIK USER's profile in the Kik app. I also reviewed the photographs that the SUSPECT KIK USER sent within the chats with the OCE. I believe that they all depict the same person.

24. On November 18, 2020, a federal search warrant was obtained to search Adams' residence for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1470. During execution of that search warrant, agents conducting a preliminary review of the SUBJECT DEVICES observed sexually-oriented chats between Adams and what appear to be numerous minor females. In reviewing these chats, agents further observed what appeared to be images constituting child pornography. Specifically, in the context of a chat between Adams and Kik user 13", who appears to be a minor female, agents observed the following:

SUSPECT KIK USER: I'd hope you'd like me me

13: I know I would because you would be the oldest I've been with that turns me on

SUSPECT KIK USER: [Smiley Face Emoji] good

SUSPECT KIK USER: I'm glad

13: I hate to sound weird but I think you would like watching a 13 year old suck your dick to

SUSPECT KIK USER: You do turn me on, I'm surprised how much

SUSPECT KIK USER: Watching…feeling would be the best part

3: I will look up at you the whole time I do it I would have sex with you too if you was comfortable with it

SUSPECT KIK USER: Well I'm sure if we were together and wanted it, I'd be comfortable

SUSPECT KIK USER: I'm 7in and a little thick btw

3: Cool because I definitely would want to I'm pretty tiny down there so Idk care if you could or not LOL [KAYYMOORE13 then sends SUSPECT KIK USER a selfie-style photograph taken at close range depicting a naked vagina with no visible pubic hair]

: Shhhh [Winking Eye Emoji]

SUSPECT KIK USER: You haven't had my size?

SUSPECT KIK USER: Mmm so yummy

13: No 6Was probably the biggest

13: And they wasnt thick

13: At all

SUSPECT KIK USER: Oh…hmm maybe we could make it work

[13 then sends SUSPECT KIK USER a selfie-style photograph taken from the chest down depicting a nude female with minimal breast development using two fingers to spread open her vagina, which has no visible pubic hair]

SUSPECT KIK USER: Mmm Kaylin is nice

13: Thx…and yeah I hope so because I would want to have sex with you for sure if you are here

[SUSPECT KIK USER then sends 13 a picture of a penis, which is consistent to photos Adams had sent to the OCE].

25. Upon observing these images, agents immediately suspended their review of Adams' devices.

26. During a voluntary interview with agents, Adams admitted to chatting online with minor females on a daily basis via multiple online platforms and sending nude photographs of himself taken on his tablet and phone to these minor females. Adams also admitted to receiving nude photographs from minor females and masturbating to them.

COMPUTERS AND FORENSIC ANALYSIS

27. Your Affiant is aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

28. Your Affiant is also aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers

of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

29. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is <u>not</u> present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

CONCLUSION

30. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crime of possession of child pornography and receipt of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) & 2252A(a)(2) may be located on the SUBJECT DEVICES. I therefore seek a warrant to search the SUBJECT DEVICES described in Attachment A for the items described in Attachment B.

/s/ Tarah Rankins
Tarah Rankins
Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Nov 19, 2020

Time: 4:07PM, Nov 19, 2020

Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

PREMISES TO BE SEARCHED

The SUBJECT DEVICES to be searched include:

1. One black Apple iPhone 7, Serial Number F71TJ2L3HG75, in a black Otter Box case with charger
2. One Microsoft Surface Pro4, Serial Number 026805763853, with charger and keyboard

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(2):

1. All records relating to violations of 18 U.S.C. §§ 2252(a)(4)(B), 2252A(a)(2) in any form wherever they may be stored or found within SUBJECT DEVICES, including:

   a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;

   b. records or information pertaining to an interest in child pornography;

   c. records or information pertaining to the possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

   d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;

   e. records or information pertaining to Kik, Chat Avenue and Google

   f. photo-editing software and records or information relating to photo-editing software;

2. For all SUBJECT DEVICES:

   a. evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES;

f. evidence of the times the SUBJECT DEVICES were used;

g. contextual information necessary to understand the evidence described in this attachment.